AP1000 Protection and Safety Monitoring System (PMS)
NRC Review Plan
Revision C

Purpose:

The purpose of this document is to propose a schedule for the review of AP1000 PMS design. Review dates are selected, where meaningful NRC reviews can be accomplished based on the NRC's plan for technical review in the instrumentation and control systems area.

A schedule of proposed human factors engineering (HFE) reviews is being prepared in a separate document.

NRC Review Process:

The NRC will confirm that the as-built computer-based plant I&C system conforms to the certified design. The design acceptance criteria will be verified to be met as part of the I&C system Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC). The ITAAC reviews will be performed by the NRC prior to fuel load at specified points in the system lifecycle.

The NRC staff will use a two-part approach for the review of the PMS as follows:

- Detailed functional review at the block diagram level to ensure appropriate implementation of NRC requirements related to postulated single failures, common-mode failures, appropriate signal isolation, and other aspects of NRC review. This review will establish the detailed functional requirements for the I&C systems.
- Review of the implementation of digital I&C systems to meet the functional system requirements. Review points will be selected based on the system lifecycle process to verify that the implementation is proceeding in accordance with the design certification. A review will be done for each phase of the I&C system software and hardware development process.

The review guidance provided in SRP Chapter 7, Rev. 4, 1997, will be used by the staff in review of the I&C system design, installation and operation. Of particular note is the guidance in Appendix 7-A, Branch Technical Position (BTP) 14, "Guidance on Software Reviews for Digital Computer-Based I&C Systems" which applies to the plant-specific software application.

Technical Review Plan:

Table 1 below provides the review schedule. It includes the proposed review date for each lifecycle phase and a list of documents that will be available for the staff's review. The list of documents is correlated with the list of reference topics provided in BTP 14, Figure 7-A-1. Review dates are specified in "Months ARO". The phase definitions identified in parenthesis in Column 2 are consistent with the Common Q design terminology.

Table 2 below defines the scope of each review with specific references to ITAACs that are included in the AP1000 Design Control Document. This table provides the details of each planned review including a cross reference of the contents of each available document with the design commitment and associated acceptance criteria that it attempts to satisfy.

Actions to Prepare for NRC Reviews:

- Review and determine how to address cyber security. This should include an evaluation of DG-1130, NEI 04-04, and NUREG/CR-6847.
- Map BTP-14 with the Common Q approved design process.
- Perform an internal audit to assess readiness prior to each scheduled NRC review.

Table 1. Review Schedule

Review Date (Months ARO)	Completion of System Lifecycle Phase	BTP 14, Figure 7-A-1 Reference Topics	Available Documents
12	Design Requirements (Concept Phase)	Software Management Plan Software Development Plan Software QA Plan Integration Plan Installation Plan Maintenance Plan Training Plan Operations Plan Software Safety Plan Software V&V Plan Software CM Plan	Software Program Manual Project Quality Plan Project Document Index Commercial Grade Dedication Plan AP1000 V&V Plan System Test Plan
26	System Definition (Requirements Analysis Phase)	Requirements Specifications Requirements Safety Analysis V&V Requirements Analysis Report CM Requirements Analysis Report	Generic Safety System Requirements AP1000 Safety System Requirements Functional Requirements System Hardware Requirements Software Requirements Specification System Interface Requirements

Table 1. Review Schedule

Review Date (Months ARO)	Completion of System Lifecycle Phase	BTP 14, Figure 7-A-1 Reference Topics	Available Documents
			Requirements Phase V&V Report Requirements Phase RTM Project Document Index
40	Hardware and Software Development, consisting of hardware and software design and implementation (Design Phase & Implementation Phase)	Design Specifications Hardware & Software Architecture Design Safety Analysis V&V Design Analysis Report CM Design Report Code Listings Code Safety Analysis V&V Implementation Analysis & Test Report CM Implementation Report	System Design Specification System Architecture Drawings Hardware Design Drawings CM Release Report Custom Software Element Design Specifications Reusable Software Type Specifications Module/Unit Test Procedures Module/Unit Test Reports BPL Software Design Description LCL Software Design Description ITP Software Design Description ILC Software Design Description MUX Software Design Description MTP Software Design Description Design and Implementation Phase V&V Reports

Table 1. Review Schedule

Review Date (Months ARO)	Completion of System Lifecycle Phase	BTP 14, Figure 7-A-1 Reference Topics	Available Documents
			Design and Implementation Phase RTM Project Document Index
TBD	System Integration and Test (Test Phase)	System Build Documentation Integration Safety Analysis V&V Integration Analysis & Test Report CM Integration Report Validation Safety Analysis V&V Validation Analysis & Test Report CM Validation Report	
TBD	Installation (Installation and Checkout Phase)	Operations Manuals Installation Configuration Tables Maintenance Manuals Training Manuals Installation Safety Analysis V&V Installation Analysis & Test Report CM Installation Report	

Table 2. May 2006 Concept Phase Review

DCD Table 2.5.2-8 ITAAC Reference	Design Commitment	Document Reference	Acceptance Criteria Satisfied
Item 11.a	PMS hardware and software is developed using a planned design process which provides for specific design documentation and reviews during the design requirements phase.		Establishment of plans and methodologies.

Comments on Draft NEI 04-01, Rev D – 4.3.9.7 FSAR Chapter 7

The implementation of the design of the plant-specific safety I&C systems is covered by the Chapter 7 DAC/ITAAC. The use of design acceptance criteria enables the staff to arrive at a safety determination regarding a specific aspect of the overall plant design. By designating the DAC in the design certification rule, the Commission will establish the criteria which the staff will utilize to confirm that the as-built plant conforms to the design certification. The determination that the DAC have been satisfied will be made throughout the design implementation and construction process, as part of ITAAC program.

The NRC staff intends to perform inspections that will audit the satisfactory completion of ITAAC requirements, including the DAC. In accordance with section 52.99, "At appropriate intervals during construction, the NRC staff shall publish in the Federal Register notices of the successful completion of inspections, tests, and analyses."

The staff will use a two-part approach for the review of advanced instrumentation and controls (I&Cs). The first part will involve a detailed, functional review at the block diagram level, to ensure appropriate implementation of NRC requirements related to postulated single failures, common-mode failures, appropriate signal isolation, and other aspects of NRC review. This review will establish the detailed functional requirements for the I&C systems.

The second part of the review will address the implementation of digital control systems to meet the functional system requirements. This will rely upon a formal process with phased ITAAC for design development. The ITAAC will all be specified in the design certification rule but could be satisfied at various points in time. An early ITAAC would address the procedures to be used by the COL holder to implement an acceptable design process for digital control systems. Acceptance criteria for the various phases of the design program would be specified, such that the NRC could objectively inspect and determine whether the licensee's procedure met the ITAAC criteria. As the design is subsequently developed and implemented, subsequent ITAAC would be used to verify key steps in the development process that have been satisfactorily accomplished. Because design detail is not available in this review area, and several design implementation methods would be acceptable to the staff, the ITAAC requirements and acceptance criteria in the design certification will be general in nature. The applicants and the NRC will establish agreed upon review points in the design development process to verify that the implementation is proceeding in accordance with the design certification.

The review guidance provided in SRP Chapter 7,Rev 4, 1997, will be used by the staff in review of the of the I&C system design, installation and operation. Of particular note is the guidance in Appendix 7-A, Branch Technical Position 14 - Guidance on Software Reviews for Digital Computer-Based I&C Systems which applies to the plant-specific software application in either the Eagle or Common Q platform. The review will be done at every life-cycle stage of the I&C system software and hardware development process. Additional guidance based on the lessons learned by using the guidance of SRP Chapter 7 in the review of computer-based I&C system design implementation at Temelin (Czech Republic -W Eagle system) and the Lungmen Project (Taiwan - twin GE ABWRs), and guidance on Cyber Security will be part of the review. The lessons learned changes are included (high-lighted) in the BTP - 14 version below ; and the discussion on cyber security items follows.

Figure 2: Software Life Cycle

Life Cycle Activity Groups	*Planning Activities*	*Requirements Activities*	*Design Activities*	*Implementation Activities*	*Integration Activities*	*Validation Activities*	*Installation Activities*	*Operations & Maintenance Activities*
	Software Management Plan *Software Development Plan* *Software QA Plan* *Integration Plan* *Installation plan* *Maintenance plan* *Training plan* *Operations Plan*	*Requirements Specifications*	*Design Specifications* *Hardware & Software Architecture*	*Code Listings*	*System Build Documentation*		*Operations Manuals* *Installation Configuration Tables* *Maintenance Manuals* *Training Manuals*	
	Software Safety Plan *Software V&V Plan* *Software CM Plan*	*Requirements Safety Analysis* *V&V Requirements Analysis Report* *CM Requirements Analysis Report*	*Design Safety Analysis* *V&V Design Analysis Report* *CM Design Report*	*Code Safety Analysis* *V&V Implementation Analysis & Test Report* *CM Implementation Report*	*Integration Safety Analysis* *V&V Integration Analysis & Test Report* *CM Integration Report*	*Validation Safety Analysis* *V&V Validation & Test Report* *CM Validation Report*	*Installation Safety Analysis* *V&V Validation & Test Report* *CM Installation Report*	*Change Safety Analysis* *V&V Change Report* *CM Change Report*

Note: A separate document is not required for each topic identified, however, project documentation should encompass all the topics.

□ *Process Planning*

□ *Design Outputs*

□ *Process Implementation*